					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P11					Asiakirjan nimi: **Käyttäjätilien ja käyttöoikeuksien hallintapolitiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 6.1.3, lauseke 8	-
ISO/IEC 27002:2022	Kontrollit 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2-IA-5, AU-2, AU-12	-
EU:n GDPR	Artiklat 5(1)(f), 32; johdanto-osan kappale 39	-
EU:n NIS2-direktiivi	Artiklat 21(2)(a, d), 21(3)	-
EU:n DORA-asetus	Artiklat 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Tarkoitus

1 Tämä politiikka määrittää pakolliset kontrollit käyttäjätilien ja käyttöoikeuksien hallinnalle kaikissa tietojärjestelmissä ja palveluissa. Se varmistaa, että pääsy organisaation resursseihin myönnetään varmennetun identiteetin, roolin edellyttämän tarpeen sekä vähimmän oikeuden periaatteen ja tehtävien eriyttämisen perusteella.

1.1 Tämä politiikka tukee organisaation sitoutumista tietoturvaan ottamalla käyttöön jäsennellyt ja todennettavat menettelyt käyttäjätilien perustamiseen, käyttöoikeuksien myöntämiseen, käytön seurantaan ja käyttöoikeuksien poistamiseen.

1.2 Tämä politiikka on keskeinen luvattoman pääsyn, käyttöoikeuksien väärinkäytön, sisäisten uhkien ja sovellettavien sääntelykehysten vastaisen toiminnan riskin vähentämisessä.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia työntekijöitä, sopimuskumppaneita, kolmansien osapuolten palveluntarjoajia, konsultteja ja muita henkilöitä, joille on myönnetty pääsy organisaation IT-resursseihin, sovelluksiin tai tietoihin.

2.2 Se koskee kaikkia järjestelmiä ja ympäristöjä, joissa sovelletaan käyttäjän todentamista ja pääsynhallintamekanismeja, mukaan lukien seuraavat:

2.2.1 yrityssovellukset ja tietokannat

2.2.2 pilvialustat ja SaaS-ympäristöt

2.2.3 käyttöjärjestelmät ja hallintakonsolit

2.2.4 etäkäyttötyökalut ja VPN-yhteydet

2.2.5 identiteetin- ja pääsynhallintajärjestelmät (IAM)

2.3 Politiikka kattaa sekä tavalliset että etuoikeutetut käyttäjätilit ja sisältää kontrollit seuraaville:

2.3.1 käyttäjätilien luominen, muuttaminen ja poistaminen käytöstä

2.3.2 käyttöoikeuksien korottaminen ja delegointi

2.3.3 istuntojen hallinta ja seuranta

2.3.4 todentamismenetelmät ja tunnistetietojen hallinta

3. Tavoitteet

3.1 Varmistaa, että kaikki käyttäjätilit ovat yksilöitävissä, asianmukaisesti valtuutettuja ja myönnetään vasta muodollisen tarpeen varmistamisen jälkeen.

3.2 Toteuttaa vähimmän oikeuden periaate ja estää tarpeeton tai liiallinen pääsy soveltamalla tiukkoja kontrolleja etuoikeutettujen tilien myöntämiseen ja käyttöön.

3.3 Edellyttää käyttäjätilien tilan oikea-aikaista päivittämistä työsuhteeseen tai rooliin liittyvien muutosten perusteella, mukaan lukien välitön poistaminen käytöstä työsuhteen päättyessä.

3.4 Mahdollistaa käyttämättömien, väärinkäytettyjen tai luvattomien käyttäjätilien ennakoivan havaitsemisen sekä korjaavat toimenpiteet lokituksen, katselmointien ja automaation avulla.

3.5 Ylläpitää yhdenmukaisuutta ISO/IEC 27001:2022 -standardin ja siihen liittyvien standardien kanssa sekä täyttää EU:n GDPR:n, EU:n NIS2-direktiivin, EU:n DORA-asetuksen ja COBIT 2019:n kaltaisten oikeudellisten ja sääntelykehysten velvoitteet.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Vastaa tästä politiikasta ja varmistaa sen toimeenpanon koko organisaatiossa.

4.1.2 Katselmoi ja hyväksyy kaikki muodolliset poikkeukset tai hätäkäyttötilanteet.

4.1.3 Raportoi käyttäjätileihin liittyvät auditointihavainnot ja eskaloi riskit ylimmälle johdolle.

4.2 Pääsynhallinnan ylläpitäjä / IT-järjestelmänvalvoja

4.2.1 Ylläpitää ja operoi käyttäjätilien elinkaaren hallinnan teknisiä kontrolleja.

4.2.2 Toteuttaa käyttöoikeuksien myöntämiseen, poistamiseen ja hallintaan liittyvät toimenpiteet hyväksyttyjen pyyntöjen perusteella.

4.2.3 Ylläpitää ajantasaista rekisteriä kaikista käyttäjätileistä, niiden tilasta ja käyttöoikeustasoista.

4.2.4 Tukee auditointeja ja vaatimustenmukaisuuden katselmointeja lokeilla ja toimintaraporteilla.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään vuosittain tai seuraavien merkittävien muutosten yhteydessä:

9.1.1 organisaatiorakenne tai liiketoimintaprosessit

9.1.2 IT-järjestelmät, identiteettialustat tai pääsymenetelmät

9.1.3 identiteetin- ja pääsynhallintaan liittyvät sääntely- tai sopimusvaatimukset

9.2 Tietoturvajohtaja (CISO) yhdessä pääsynhallinnan ylläpitäjän kanssa vastaa katselmointiprosessin käynnistämisestä ja sidosryhmäpalautteen koordinoinnista.

9.3 Katselmointeja voidaan käynnistää myös seuraavien perusteella:

9.3.1 käyttäjätilien väärinkäyttöön liittyvät tietoturvapoikkeamat

9.3.2 auditointihavainnot, jotka tuovat esiin puutteita käyttäjätilien elinkaaren hallinnassa

9.3.3 uusien identiteetin- tai etuoikeutetun pääsyn hallinnan työkalujen käyttöönotto

9.4 Tähän politiikkaan tehtävien päivitysten on oltava:

9.4.1 versiohallittuja ja tallennettu ISMS-dokumentaatiokirjastoon

9.4.2 viestittyjä kaikille olennaisille sidosryhmille, mukaan lukien osastojen johtajat, IT-operaatiot ja henkilöstöhallinto

9.4.3 tuettuja päivitetyllä koulutusmateriaalilla ja menettelyohjeilla

9.5 Kaikki muutokset on hyväksyttävä ylimmän johdon tai tietoturvan ohjausryhmän toimesta, ja ne on kirjattava lokiin auditointitarkoituksia varten.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka liittyy operatiivisesti seuraaviin ISMS-kokonaisuuden politiikkoihin ja saa niistä tukea:

10.1.1 P4 Pääsynhallintapolitiikka: määrittää yleiset pääsynhallinnan periaatteet ja mekanismit, mukaan lukien sääntöpohjaiset ja roolipohjaiset kontrollit.

10.1.2 P7 Perehdytys- ja työsuhteen päättämispolitiikka: määrittää menettelyvaiheet käyttäjän käyttöoikeuksien käynnistämiseen ja päättämiseen henkilöstöhallinnon toimien mukaisesti.

10.1.3 P8 Tietoturvatietoisuus- ja koulutuspolitiikka: vahvistaa käyttäjän vastuut käyttäjätilien turvallisuudesta ja tunnistetietojen suojaamisesta.

10.1.4 P13 Tiedon luokittelu- ja merkintäpolitiikka: ohjaa käyttöoikeustasoja tiedon luokittelun perusteella varmistaen, että käyttöoikeusrajat vastaavat tiedon arkaluonteisuustasoja.

10.1.5 P22 Lokitus- ja valvontapolitiikka: varmistaa, että kaikkiin käyttäjätileihin liittyviin toimiin muodostuu auditointijälki ja että niitä katselmoidaan poikkeamien tai luvattoman käytön havaitsemiseksi.

10.1.6 P30 Tietoturvapoikkeamien hallintapolitiikka: ohjaa eskalointia, rajaamista ja poikkeaman jälkeisiä toimia käyttöoikeuksien väärinkäytön tai luvattoman käyttäjätilitoiminnan tapauksissa.

10.2 Nämä politiikat muodostavat yhdessä johdonmukaisen, riskiperusteisen identiteetin- ja pääsynhallinnan viitekehyksen koko organisaatiossa.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisesti tunnustettujen kyberturvallisuusstandardien ja sääntelykehysten kanssa, jotka edellyttävät turvallista identiteetin, pääsyn ja käyttöoikeuksien hallintaa organisaation tietoturvan keskeisenä osana.

11.2 ISO/IEC 27001:

11.2.1 Lauseke 6.1.3 edellyttää, että organisaatiot tunnistavat, arvioivat ja käsittelevät tietoturvariskejä, jolloin pääsyn ja käyttöoikeuksien hallinta muodostaa muodollisen, riskiperusteisen kontrollin osana ISMS:n suunnitteluprosessia.

11.2.2 Lauseke 8.1 - operatiivinen suunnittelu ja ohjaus: vahvistaa sellaisten teknisten ja menettelyllisten suojatoimien toteutusta, jotka ohjaavat käyttäjien ja etuoikeutetun pääsyn hallintaa.

11.3 ISO/IEC 27002:2022 - kontrollit 5.15-5.18:

11.3.1 Kontrolli 5.15 - käyttäjien käyttöoikeuksien hallinta: tukee muodollisia menettelyjä käyttäjätilien perustamiseen, käyttöoikeuksien valtuuttamiseen ja käyttöoikeuksien säännölliseen katselmointiin.

11.3.2 Kontrolli 5.16 - identiteetinhallinta: määrittää identiteetin yksilöllisyyden, elinkaarikontrollit ja turvallisen todentamisen toteutuksen.

11.3.3 Kontrolli 5.17 varmistaa, että etuoikeutettujen käyttöoikeuksien myöntämistä ja käyttöä hallitaan tiukasti, ne ovat jäljitettävissä ja yhdenmukaisia vähimmän oikeuden periaatteen kanssa koko käyttäjätilin elinkaaren ajan.

11.3.4 Kontrolli 5.18 - käyttöoikeudet: katetaan täysimääräisesti roolipohjaisella käyttöoikeuksien myöntämisellä, auditoinnilla ja korotettujen käyttöoikeuksien hyväksyntävaatimuksilla.

11.4 Nämä kontrollit ohjaavat käyttäjätilien rekisteröinnin, rekisteristä poistamisen, käyttöoikeuksien eriyttämisen ja todennustietojen käytön jäsenneltyä toteutusta. Tämä politiikka toimeenpanee identiteetin elinkaaren hallinnan, just-in-time-pääsyn ja korotettujen istuntojen seurannan luvattoman järjestelmäkäytön estämiseksi.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (pääsynhallintapolitiikka) ja AC-2 (käyttäjätilien hallinta): toteutuvat tämän politiikan vaatimuksissa käyttöoikeuksien hyväksynnöistä, roolituksesta ja käyttäjätilien auditoinnista.

11.5.2 AC-5 (tehtävien eriyttäminen) ja AC-6 (vähimmän oikeuden periaate): toteutuvat käyttöoikeuksien rajaamisella, työroolien mukaisuudella ja kahden hyväksyjän menettelyllä korkean riskin tehtävissä.

11.5.3 IA-2-IA-5 (tunnistaminen ja todennus): toteutuvat vahvojen todennusmekanismien, tunnistetietojen elinkaarisääntöjen ja MFA-vaatimusten kautta.

11.5.4 AU-2, AU-12 (auditointilokitus ja analyysi): toteutuvat istuntojen tallennuksen ja etuoikeutettujen toimintojen seurannan kautta arkaluonteisissa ympäristöissä.

11.6 EU:n GDPR (2016/679):

11.6.1 Artikla 32 - käsittelyn turvallisuus: edellyttää pääsynhallinnan kontrolleja ja identiteetin varmennusmekanismeja henkilötietojen suojaamiseksi. Tämä toteutuu vaatimalla käyttäjätilien hyväksyntöjä, käyttöoikeuksien katselmointeja ja vahvaa tunnistautumista.

11.6.2 Artikla 5(1)(f) - eheys ja luottamuksellisuus: varmistaa, että henkilötietoihin pääsevät vain valtuutetut käyttäjät, joilla on oikeutettu rooli; tätä tuetaan käyttäjätilien hallinnan soveltamisella.

11.6.3 Johdanto-osan kappale 39: edellyttää selkeää pääsyn rajoittamista ja osoitusvelvollisuutta; tämä politiikka tukee käyttäjäidentiteettien ja käyttöoikeuksien myöntämisten täyttä jäljitettävyyttä.

11.7 EU:n NIS2-direktiivi (2022/2555):

11.7.1 Artikla 21(2)(a, d): edellyttää, että toimijat soveltavat pääsynhallintapolitiikkoja sekä suojaavat tunnistetietojen ja etuoikeutettujen istuntojen käsittelyn. Tätä tuetaan tässä politiikassa käyttöoikeuksien myöntämistä, seurantaa ja poikkeuksia koskevilla kontrolleilla.

11.7.2 Artikla 21(3): edistää pääsyn kurinalaista hallintaa ja vahvaa identiteetin varmistamista kriittisillä toimialoilla; tämä toteutuu yksilöllisten tunnisteiden, roolipohjaisen käyttöoikeuksien hallinnan ja määräaikaisten korotettujen käyttöoikeuksien kautta.

11.8 EU:n DORA-asetus (2022/2554):

11.8.1 Artikla 5 - ICT-hallinnointi ja -kontrolli: edellyttää muodollisia ICT-käyttäjähallinnan menettelyjä, jotka katetaan dokumentoidulla käyttöoikeuksien myöntämisellä, poistamisella käytöstä ja poikkeusten käsittelyllä.

11.8.2 Artikla 9 - ICT-riskien hallinta: ohjaa organisaatioita suojaamaan järjestelmät pääsyn rajoittamisella ja seurannalla; tämä toteutuu MFA:lla, etuoikeutettujen käyttöoikeuksien lokituksella ja keskitettyjen katselmointien avulla.

11.9 COBIT 2019:

11.9.1 DSS01 - hallitut operaatiot: edistää standardoitujen operatiivisten kontrollien soveltamista, mukaan lukien käyttäjätilien elinkaaren hallinta ja pääsyn dokumentointi.

11.9.2 DSS05 - hallitut tietoturvapalvelut: koskee käyttäjien ja järjestelmien käyttöoikeuksien turvallista hallintaa ja tukee riskien lieventämistä vähimmän oikeuden periaatteen ja auditointijäljen validoinnin avulla.

11.9.3 APO13 - hallittu tietoturva: edellyttää pääsyn hallinnointia digitaalisille omaisuuserille, mikä toteutuu muodollisilla käyttäjätilien ja roolien valtuutusmenettelyillä sekä määräaikaisilla katselmointivaatimuksilla.